IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NORTH DAKOTA

UNITED STATES OF AMERICA, Plaintiff, v. NICHOLAS JAMES MORGAN-DEROSIER, Defendant.	Case No. 3:22-cr-05 **UNITED STATES' POST-HEARING BRIEF ON DEFENDANT'S MOTION TO SUPPRESS EVIDENCE**

The United States of America, by Mac Schneider, United States Attorney for the District of North Dakota, and Jennifer Klemetsrud Puhl, First Assistant United States Attorney, and Charles Schmitz, Trial Attorney, United States Department of Justice, hereby files this Post-Hearing Brief in Opposition to Defendant Nicholas James Morgan-Derosier's Motion to Suppress. (Doc. 70.) For all the briefing, testimony, and exhibits introduced in these proceedings, the Court's decision can be reduced to two issues:

1. Does the plain view doctrine apply?
2. If the plain view doctrine does not apply, does the inevitable discovery doctrine apply?

There are, of course, multiple sub-issues subsumed within the plain view analysis (a doctrine the Defendant does not even cite in his brief). But the plain view elements should provide the court's framework for its decision. For reasons that follow, both the plain view doctrine and the inevitable discovery doctrine apply in this case.[1]

[1] The United States has already briefed many of the issues, and we will not repeat that briefing here. Instead, we hereby incorporate that briefing by reference. (See Docs. 77, 88.) The United States files this

I. The Plain View Doctrine Applies Here

Under the plain-view doctrine, law enforcement is permitted "to seize evidence without a warrant when (1) the officer did not violate the Fourth Amendment in arriving at the place from which the evidence could be plainly viewed, (2) the object's incriminating character is immediately apparent, and (3) the officer has a lawful right of access to the object itself." United States v. Alexander, 574 F.3d 484, 490 (8th Cir. 2009).

Here, the elements of the plain view doctrine are met. First, officers did not violate the Defendant's Fourth Amendment rights "in arriving at the place from which evidence could be plainly viewed" because they searched the thumb drive upon which they found the image pursuant to a valid search warrant that authorized the search for, *inter alia*, "visual depictions of projects, job sites, communications, account data, timesheet information, customer information," and for "[r]ecords evidencing ownership of digital media devices and removable storage." (Gov't Hr'g Ex. 13 at 2.) Second, the object's incriminating character – child sexual exploitation materials (CSAM) – was immediately apparent. Third, the officers had a lawful right of access to the CSAM because, again, they searched pursuant to, and within the scope of, a valid warrant. Moreover, even if the warrant was somehow not valid for any reason, the officers obtained and executed the warrant in good faith. These elements are addressed below.

brief only to supplement its prior briefing with evidence from the record that was introduced at the hearing.

A. There is no "Fourth Element" to the Plain View Analysis that Requires "Inadvertence," and Even if There was, GFPD Intended to Search the Thumb Drive for Illegal Business Activity

Although he fails to re-raise this argument in his post-hearing brief, most of the Defendant's questioning at the hearing, and the focus of his pre-hearing briefing, is devoted to a concept that is not even relevant – law enforcement intent. The Defendant proposes the Court read into the plain view doctrine a requirement that law enforcement have no knowledge or suspicion that there may be evidence of other crimes found in plain view. The United States has previously briefed and argued that there is no "inadvertence" element, so it will not re-brief it here. (See Doc. 88 at 7-11.); see also Maryland v. Garrison, 480 U.S. 79, 84 (1987) (holding that the scope of a search conducted pursuant to a warrant is defined objectively by the terms of the warrant and the evidence sought, not by the subjective motivations of an officer); Whren v. United States, 517 U.S. 806, 813 (1996) ("Subjective intentions play no role in ordinary, probable-cause Fourth Amendment analysis"); see also United States v. Williams, 592 F.3d 511, 522–23 (4th Cir. 2010); United States v. Stabile, 633 F.3d 219, 240 (3d Cir. 2011).[2] The Defendant's proposed addition to the plain view analysis would lead to absurd results, namely, that if law enforcement suspects that the Defendant might have incriminating evidence on his computer of "Crime A," then he would be immunized – permanently –

[2] See also United States v. Suing, 712 F.3d 1209, 1212 (8th Cir. 2013); United States v. Koch, 625 F.3d 470, 476 (8th Cir. 2010); United States v. Hudspeth, 459 F.3d 922, 928 (8th Cir. 2006), reh'g en banc granted, opinion vacated (Jan. 4, 2007), opinion reinstated in part on reh'g, 518 F.3d 954 (8th Cir. 2008) United States v. Alexander, 574 F.3d 484, 490 (8th Cir. 2009) (rejecting similar arguments to the one the defendant raises here).

for the evidence of "Crime A" found on that computer during a lawful search of the computer for evidence of a different crime, "Crime B."

Even if there was an "inadvertence" requirement, the evidence shows GFPD did, in fact, find the CSAM inadvertently. It is unclear who's intent would "matter" under the Defendant's newly proposed "inadvertence" element, but to the extent Detective Buzzo's intent is relevant, there was no evidence at the hearing that Detective Buzzo used his fraud investigation as a "stalking horse" for a CSAM investigation. The investigation came in as a wholly unrelated check fraud matter from a complainant – Dawn Peterson. (Hr'g Tr. Vol. I at 14.) Detective Buzzo was assigned the matter through the normal course of his financial crime duties. (Hr'g Tr. Vol. I at 15.) He was not even aware of the Cybertip when he first sought to clear Peterson's complaint eight months after she reported it to the GFPD. (Hr'g Tr. Vol. I at 17; Vol. II at 201.) It was not until a later coincidental conversation with Detective Freeman about Defendant's address that Detective Buzzo first became aware of the Cybertip and Detective Freeman's inactive CSAM investigation. (Hr'g Tr. Vol. I at 25-26.) This conversation was "[m]aybe a minute, a little bit more, a little bit less, give or take." (Hr'g Tr. Vol. II at 201.) In fact, Detective Buzzo mentioned "Team Lawn" to Detective Freeman, and not vice versa. (Hr'g Tr. Vol. I at 25.)

Subsequently, Detective Buzzo contacted the North Dakota Attorney General's Consumer Protection Office (Hr'g Tr. Vol. I at 16), located job postings for Defendant's business (Hr'g Tr. Vol. I at 23-24; Gov't Hr'g Ex. 4), interviewed Defendant's customers (Hr'g Tr. Vol. I at 26, 29, 58-60), investigated and photographed a jobsite (Hr'g Tr. Vol.

I at 27; Gov't Hr'g Exs. 6(a)-6(j)), ran the registration for vehicles located at the jobsite (Hr'g Tr. Vol. I at 29), obtained and executed a search warrant for Team Lawn's bank account (Hr'g Tr. Vol. I at 53), and interviewed Defendant's employees, both former and current. (Hr'g Tr. Vol. I at 33, 41-46.) In addition, Detective Buzzo interviewed Defendant on two occasions, first at a jobsite on August 25, 2020, and again at his residence on September 15, 2020. (Hr'g Tr. Vol. I at 38-41, 104-105, 110.) Both these interviews lasted roughly one hour, during which Detective Buzzo never once asked him questions about the Cybertip or the closed CSAM investigation. (Hr'g Tr. Vol. I at 38, 110.) Rather, the recorded interviews reflect that Detective Buzzo's focus was the financial crimes; namely, construction fraud, violation of the Injunction, and Defendant's operating a contracting business without a license. (Gov't Hr'g Exs. 73-75.) Accordingly, there can be no doubt that there was a bona fide investigation into Team Lawn and that the affidavit itself provided sufficient probable cause that Defendant committed the three crimes alleged therein. (Gov't. Hr'g Ex. 13.)

To the extent Detective Freeman's intent is relevant, there is similarly no evidence that Detective Freeman was "pulling the strings" of the "Team Lawn" investigation. The Defendant suggests that something nefarious was afoot even by Detective Freeman's assignment to the search warrant in the first instance – a theory that was thoroughly debunked by the evidence at the hearing that Detective Freeman was the only forensic technician at GFPD who performs digital extractions and analysis of computers on *all* investigations, including illegal business activities. (Hr'g Tr. Vol. I at 81; Hr'g Tr. Vol. II at 254-255.) Moreover, the uncontroverted testimony was that, due to the size of the

Department, GFPD detectives all generally "team up" on search warrants and have "all hands-on deck." (Hr'g Tr. Vol. I at 79-80; Hr'g Tr. Vol. II at 276-77.) Moreover, officers located the Lexar thumb drive that contained some of Defendant's CSAM from a safe chocked full of documents labelled for the Defendant's lawn service business (not for "child pornography"). (See Hr'g Tr. Vol. II at 285; Gov't Hr'g Exs. 55, 56 (showing pictures of the safe with "Team Lawn" documents.)) After hooking up the larger hard drive to be imaged, Detective Freeman went on to the smaller thumb drives. (Hr'g Tr. Vol. II at 291-92.) Detective Freeman opened the thumb drive that was in the "Team Lawn" safe first and opened the "Klein" file. (Hr'g Tr. Vol. II at 306.) If she was specifically looking for CSAM, there were other files with names that were far more indicative of CSAM then "Klein." (See Gov't Hr'g Ex. 79 at 2 (showing that the Defendant possessed files labelled "My Favourite Butts," and "Boy on Bed.")) She had no idea what was in the Klein file before she opened it, nor could she. (Hr'g Tr. Vol. II at 306.) Regardless of whether she suspected the file would contain CSAM, she would have needed to open that file anyway to comply with the search warrant, which directed her to search for, *inter alia*, "visual depictions of job sites." (Gov't Hr'g Ex. 13 at 2.) Indeed, the Defendant's own forensic expert testified that he would have opened those exact same files if he were tasked with completing the same search. (Hr'g Tr. Vol. II at 435-36.)

But again, for reasons set forth in our previous brief (Doc. 88 at 7-11), Detective Buzzo's, Detective Freeman's, or any other law enforcement official's subjective intent when they executed a search warrant is irrelevant.

B. Officers did not Exceed the Scope of the Warrant

Again, the warrant authorized the search for, *inter alia*, "visual depictions of projects, job sites, communications, account data, timesheet information, customer information," and for "[r]ecords evidencing ownership of digital media devices and removable storage." (Gov't Hr'g Ex. 13 at 2.) The Klein files - .jpg files – are plainly "visual depictions" and "records evidencing ownership of the digital media." There is no straight-faced argument that the warrant did not authorize the search of the Klein files. Therefore, officers did not exceed the scope of the search.

C. The Warrant Established Probable Cause to Search the Klein Files

The Defendant argues that "[o]fficers lacked probable cause to believe Mr. Morgan-Derosier stored business records as images or videos, or that any files predated 15 October 2019." (Doc. 109 at 2.) It thus appears that the Defendant raises two objections that are both without merit. First, he argues that the warrant failed to establish probable cause to search any files created before October 15, 2019, and second that there was no probable cause to search image files, but rather, only things like excel spreadsheets or QuickBooks files. Those arguments are addressed in turn.

1. The "Magic-Cutoff-Date" Argument is Without Merit

The Defendant's argument that there is no probable cause to search files that "predate October 15, 2019" is wholly without merit for one particularly glaring reason - the files that the Defendant claims were illegally searched – the "Klein" files – had created dates ***after*** **October 15, 2019**. (See Gov't Hr'g Ex. 91 at 2 (showing that the Klein files were "created" on **September 7, 2020**).) So even if the Defendant is correct

and the affidavit failed to provide probable cause to search documents that predated October 15, 2019, there would still be probable cause to search the "Klein" files because those files postdate October 15, 2019.[3] Knowing this, it is difficult to see how the Defendant persists in this argument in good faith.

But even if the Klein files did "predate" October 15, 2019, which they don't, the affidavit still established probable cause to search those files anyway. First, the warrant not only authorizes the search for business documents, but also evidence of attribution. (See Gov't Hr'g Ex. 13 at 2 ("[r]ecords evidencing ownership of digital media devices and removable storage.").) In other words, the United States would need to prove the Defendant owned, and used, the device. Image files on those devices, no matter when stored, would plainly be relevant. Indeed, the Defendant would be the first to file motions for sanctions and for Brady violations if the United States ***didn't*** review those files and they showed someone else besides the Defendant owned or used the devices.[4] Second, as

[3] To the extent that the Defendant argues that the entire warrant was invalid because it lacks probable cause to support part of it (i.e. that only the part that authorized the search of files that pre-date October 15, 2019, is invalid), that argument is without merit because warrants are severable. United States v. Pitts, 173 F.3d 677, 681 (8th Cir. 1999) ("A court can sever deficient portions of a search warrant without invalidating the entire warrant.") See also United States v. Fitzgerald, 724 F.2d 633, 637 (8th Cir.1983) (en banc). ("[W]e hold that the infirmity of part of a warrant requires the suppression of evidence seized pursuant to that part of the warrant (assuming such evidence could not otherwise have been seized, as for example on plain-view grounds during the execution of the valid portions of the warrant), but does not require the suppression of anything described in the valid portions of the warrant (or lawfully seized—on plain view grounds, for example—during their execution).")

Similarly, the Defendant argues "[o]fficers did not have probable cause to search for contraband or 'other items illegally possessed.'" (See Doc. 109 at 5.) This argument is a red herring, but even if it wasn't, again, it would be without merit because that portion of the warrant would be severable even if unsupported by probable cause. See Pitts, 173 F.3d at 681; Fitzgerald, 724 F.2d at 637.

[4] The Defendant proposes a largely uncited hypothetical in his motion about the search of a phone for evidence of a "failure to appear" crime. The hypothetical is misleading for a few reasons. First, it splices

previously briefed, evidence related to the Defendant's conduct of the lawn service before the Defendant's "magic cutoff date" is relevant to show he continued his business after that date. (See U.S. Response to Motion to Suppress, Doc. 77 at 23-25; Gov't Hr'g Ex. 13 (establishing that businesses keep their records stored).) Moreover, the search warrant was not limited to a search for files containing evidence of the violation of the court order. Rather, it also authorized officers to look for evidence of construction fraud and operating a contracting business without a license, both crimes that predated the

---

one Fourth Amendment concept – "whether a defendant has a reasonable expectation of privacy" – onto another Fourth Amendment concept – "whether a warrant is supported by probable cause." No one is arguing that the defendant did not have a reasonable expectation of privacy in his thumb drive, or that law enforcement officers did not need a warrant here. They did, and they got one.

Second, there are other critical distinctions between the defendant's hypothetical and this case that make it inapposite. (Doc. 99 at 2-3.) For example, the Defendant's hypothetical starts from the assumption that the government can prove the individual owns the phone. The United States cannot anticipate what the defendant's defense will be in this case, of course, but in most crimes that defendants commit with digital devices, the only real defense to the crime is some version of "SODDI" (some other dude did it). That requires the United States prove the defendant's ownership and/or use of the device. In those cases, a defendant's camera roll that shows 800 "selfies" is good evidence of who owns the device.

There are other false equivalencies in the hypothetical. The defendant articulates a search of a phone and not a thumb drive. Moreover, the Defendant's hypothetical contemplates the search for evidence of an individual's location over a few hours, whereas this case involved the search for business records and other evidence to show the Defendant committed three different crimes over, at a minimum, months. Additionally, the only case he cites – Riley – involved a warrantless search, whereas here, there was a warrant.

Finally, the defendant's hypothetical attempts to "scare" the court into a post-hoc review not of whether the warrant was supported by probable cause or otherwise sufficiently particular, but rather, whether the defendant's reasonable expectation of privacy in a large digital device should "trump" the finding of probable cause because there may be many other items on the device besides evidence of the crimes. That is not the law. When looking for a "needle" in the digital "haystack," the digital haystack is almost always very large, and sometimes the needles are very small. The question for the court is not whether the haystack is too big, or the needle too small, however. When reviewing a warrant, there is no heightened probable cause standard for a hard drive that is one terabyte, rather than one megabyte. In addition, the existence of personal documents or correspondence mixed in with contraband would not trump the probable cause – indeed, almost all cell phones have personal data on them, and indeed, sometimes the evidence *is* the personal data. One could imagine the problems that would arise if the courts had to engage in a case-by-case analysis of whether a defendant's personal expectation of privacy in a given device trumps the probable cause.

October 15, 2019, Injunction. In fact, the district court issued the injunction because the Attorney General's Consumer Protection Office alleged that it received complaints from customers that Defendant had accepted money for projects that he either did not start or complete and Defendant had made misrepresentations about having a contractor's license, when in reality he had no such license. (Hr'g Tr. Vol. II at 203-204.)

Finally, the Defendant failed to establish at the hearing any practical way to restrict the search of the files on thumb drive by date. In fact, his own expert testified that the only way he suggested, a timeline analysis, would omit potentially critical evidence like deleted documents in a computer's unallocated space, .pst files, and other forensic artifacts. (Hr'g Tr. Vol. II at 437-39.) In short, to find the needles, law enforcement must look through the relevant haystacks. Warrants therefore authorize the search of haystacks to find the needles, not just to search stacks of needles.

2. The "Images-Aren't-Evidence-of-Business-Activity" Argument is also Without Merit

The Defendant argues that the affidavit failed to establish probable cause that images could be evidence of business activity. Yes, it did. If common sense was not enough (which it is here), the affidavit spells it out in detail - "computers and the Internet has greatly changed and added to the way in which people keep records. Computers have facilitated the ability of people to keep their records stored and hidden. **Photographs, videos, and other records that were previously stored in boxes are now collected as digital images** and files that can be stored and maintained on electronic media." (Gov't Ex. 13 at 9 ¶ 17.) The Defendant counters that this is somehow "not good enough,"

because the United States needs to show before it searches a device the specific documents/images for which it is looking (i.e. "a picture defendant took of Mrs. Jones' lawn, saved as a .jpg file on xx/xx/20.") That is obviously not the standard for a search warrant, nor is it how probable cause works. See United States v. Ulbricht, 858 F.3d 71, 101 (2d Cir. 2017) (holding that a warrant is sufficiently particular if it "lists the charged crimes, describes the place to be searched, and designates the information to be seized in connection with the specified offenses."); see also United States v. Smith, 2019 WL 6117794, at *8 (E.D. Mo. Sept. 17, 2019), report and recommendation adopted 2019 WL 6115204 (E.D. Mo. Nov. 18, 2019) ("As the Second Circuit held in Ulbricht, in connection with searches of computers, 'it is important to bear in mind that a search warrant does not necessarily lack particularity simply because it is broad.' Moreover, in words equally relevant here, the Second Circuit stated that 'it will often be impossible to identify in advance the words or phrases that will separate relevant files or documents before the search takes place, because officers cannot readily anticipate how a suspect will store information related to the charged crimes.'")

Second, even if the affidavit did not establish probable cause that image files were relevant to the investigation, which it did, the warrant also provided probable cause that law enforcement would find evidence of attribution. See also United States v. Solomon, 432 F.3d 824, 827 (8th Cir. 2005) ("The affidavit "should be examined under a commonsense approach and not in a hypertechnical fashion.") It is common sense that images on one's device can prove who owns, or who used the device.

D. Good Faith Applies Here

Even if the warrant was insufficient, officers executed the warrant in good faith. The United States already briefed this issue, so it will not repeat that briefing. (Doc. 77 at 33-35.) It bears repeating, however, that there are only four circumstances that preclude a finding of good faith:

> (1) when the affidavit or testimony in support of the warrant included a false statement made knowingly and intentionally or with reckless disregard for its truth, thus misleading the issuing judge; (2) when the judge "wholly abandoned his judicial role" in issuing the warrant; (3) when the affidavit in support of the warrant was "so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable," and (4) the warrant is "so facially deficient" that the executing officer could not reasonably presume the warrant to be valid.

United States v. Grant, 490 F.3d 627, 632-3 (8th Cir. 2007) (citing United States v. Leon, 468 U.S. 897, 923 (1984)).

The Defendant takes a scattershot approach to his lack of good faith argument. First, he recycles his particularity argument and asserts that the warrant "[f]ail[s] to include time limits on the warrant." As an initial matter, it did provide dates of the offenses (Gov't Hr'g Ex. 13 ¶¶ 5-10, 14), and the Defendant himself (erroneously) argues, elsewhere in his brief, that officers failed to comply with those dates when it purportedly searched files that pre-dated October 15, 2019 (the Klein files did ***not*** pre-date October 15, 2019). Moreover, all of the "magic cutoff date" arguments above apply here. See supra at C.1.

Next, the Defendant makes a choice-of-language argument. Specifically, he suggests, again, something nefarious must have been afoot because some of the language

that Detective Buzzo used in his warrant to describe visual images often appears in CSAM investigations. (Doc. 109 at 8.) It is unclear, however, how the use of the words "possession, receipt, and distribution," and "visual depictions" are not just effective language to use when searching for images of any kind, CSAM or otherwise. Perhaps the argument goes that, if Detective Buzzo had no nefarious intent, he would have re-created the wheel, opened a thesaurus, and come up with different words to describe computer images that were different than the language that works well in CSAM investigations.

Putting that to the side, this argument is without merit for at least a few other reasons: (1) it doesn't meet any of the four circumstances above that would preclude a finding of good faith; (2) Detective Buzzo's (or any other law enforcement officer's) subjective intent, legally, doesn't matter anyway; see supra I.A., and (3) even if it did matter, which it doesn't, the evidence showed probable cause that the Defendant defrauded customers and employees. (See Gov't Hr'g Ex. 13 ¶¶ 11, 12 (outlining how the Defendant failed to pay employees); Gov't Hr'g Ex. 13 ¶ 13 (outlining how Defendant ripped off at least one of his customers).) In fact, even the testimony at the hearing further corroborated that there was probable cause that the Defendant engaged in check fraud – the allegation that sparked the illegal business investigation to begin with. (Hr'g Tr., Vol. I at 88, 112 (indicating that the Defendant wrote checks on behalf of a business partner that Defendant killed when he ran him over with a "Bobcat" machine).)

Defendant's other "lack of good faith" arguments are similarly without merit. The evidence at the hearing debunked his claim that the execution of the search warrant was strategically staffed with CSAM investigators while Detective Buzzo was outside. (See

Hr'g Tr. Vol. II at 208, 255 (Detective Freeman was assigned to the search warrant because she was the only forensic tech at GFPD who analyzes hard drives for any type of crime, and because warrants are "all hands-on deck"); Hr'g Tr. Vol. II at 370-71, 384-85 (showing that Agent Casetta participated in the Search Warrant for manpower and was a drug task force officer who had never led a CSAM investigation in his life to that point).

Moreover, the Defendant cites Detective Freeman's failure to use a "write blocker," which is, at best, an issue related to authentication of evidence. But there is no issue. The Defendant proved nothing other than that the "last accessed dates" were unintentionally altered. No other data was altered. (Hr'g Tr. Vol. II at 364.) So the "write-blocker" issue is largely irrelevant for this entire case, let alone on a motion to suppress. But perhaps more to the point, none of these arguments relate in any way to the four circumstances mentioned above that would preclude a finding of good faith mentioned above.

II. Inevitable Discovery Would Apply Here Even if the Plain View Doctrine Does Not

Even if the Plain View Doctrine does not apply here (which it does), law enforcement officers would have inevitably discovered CSAM on the Defendant's Devices. The United States articulated this argument in greater detail in its prior briefing, and we will not repeat it here. (See Doc. 88 at 3-7.) The United States writes only to outline the evidence introduced at the hearing that supported this argument. Specifically, the Defendant possessed 6,097 files of CSAM on more than four different devices. (Hr'g

Tr. Vol. II at 312-314.[5]) In fact, the tower computer that the Defendant admitted he used for work purposes, and the thumb drive that was plugged in to the Defendant's work tower, *both* had CSAM on them. (Hr'g Tr. Vol. II at 311-312.) It can hardly be disputed that, if the United States was looking for visual depictions of job sites, or for evidence of attribution, the United States would have found at least some of those six thousand-plus images of children being sexually abused.

IV. CONCLUSION

For the preceding reasons, and for reasons previously briefed, the Court should deny the Defendant's Motion to Suppress.

Dated: June 7, 2023

MAC SCHNEIDER
United States Attorney

By: */s/ Jennifer Klemetsrud Puhl*
JENNIFER KLEMETSRUD PUHL
Assistant United States Attorney
ND Bar ID 05672
655 First Avenue North, Suite 250
Fargo, ND 58102-4932
(701) 297-7400
jennifer.puhl@usdoj.gov
Attorney for United States

By: /s/ Charles Schmitz
CHARLES SCHMITZ
Trial Attorney
Criminal Division
U.S. Department of Justice
(202) 913-4778
Charles.Schmitz2@usdoj.gov

[5] The United States anticipates that the evidence at trial will show the Defendant possessed CSAM on more than just those four devices.